Number: CSB-160115-1

Released: 15th Jan 2016

Modified:

Subject: FortiOS SSH Undocumented Interactive Login Vulnerability

Product: FortiGate

Description:

A device management authentication vulnerability exists in earlier builds of FortiOS which could allow unauthorized users to obtain remote console access to vulnerable devices when "Administrative Access" is enabled for SSH.

Possibly Affected Products:

All FortiGate models running the following FortiOS versions
FortiOS 4.3.0 to 4.3.16
FortiOS 5.0.0 to 5.0.7

Remedy:

FortiOS branch 4.3: Upgrade to FortiOS 4.3.17 or later

FortiOS branch 5.0: Upgrade to FortiOS 5.0.8 or later

Workarounds:

Disable admin access via SSH on all interfaces, and use the Web GUI instead, or the console applet of the GUI for CLI access.

```
config system interface
edit <interface name>
set allow  < management protocols ..... do not include ssh >
```

If SSH access is mandatory, in 4.3 and 5.0 you can restrict access to SSH to a minimal set of authorized source IP addresses, via the Local In Policy feature, an example can be found below:

Sample syntax in FortiOS 4.3 and 5.0:

```
# SSH Access permitted for allowed host addresses
config firewall local-in-policy
   edit 1
      set intf  <interface>
      set srcaddr <address objects for allowed host addresses>
      set dstaddr "all"
      set action accept
      set service "SSH"
      set schedule "always"
   next

# SSH Access denied for all other host IP addresses
   edit 2
      set intf <interface>
      set srcaddr "all"
      set dstaddr "all"
      set service "SSH"
      set schedule "always"
   end
```

For future updates, please consult the following FortiGuard advisory:
http://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability

Technical Support Contact Information:
http://www.fortinet.com/support/contact_support.html
Fortinet technical support home page: https://support.fortinet.com

All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Statements contained herein were attained in internal lab tests under ideal conditions, and performance may vary; network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment or admission of fault by Fortinet, and Fortinet disclaims all representations and warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with an express representation or warranty included therein. All Fortinet end-customers are bound by the terms of Fortinet's current End User License Agreement. The information in this Customer Support Bulletin is provided for remedial purposes and is designed to assist customers in corrective action that may be helpful to the customer.